



PC/2098/00181

PC'D 16 SEP 1998

WIPO

PC



РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)
ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

09/622048520

рег. No 20/14-347(2)

11 августа 1998 года

СПРАВКА

Федеральный институт промышленной собственности Российского Агентства по патентам и товарным знакам настоящим удостоверяет, что приложенные материалы являются точным воспроизведением первоначального описания, формулы и чертежей (если имеются) заявки на выдачу патента на изобретение N 98104851, поданной в марте месяце 20 дня 1998 года.

Название изобретения: Способ блочного шифрования дискретной информации.

Заявитель (и): МОЛДОВЯН Александр Андреевич.

Действительные авторы: МАСЛОВСКИЙ Владимир Михайлович,
МОЛДОВЯН Александр Андреевич,
МОЛДОВЯН Николай Андреевич.

**PRIORITY DOCUMENT**

Уполномоченный заверить копию
заявки на изобретение

Г.Ф.Востриков
Заведующий отделом

Экз. N

МПК⁶ H 04 L 9/00

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации). В совокупности признаков заявляемого способа используются следующие термины:

- секретный ключ представляет из себя комбинацию битов, известную только законному пользователю;

- ключ шифрования представляет из себя комбинацию битов, используемую при шифровании информационных сигналов данных; ключ шифрования является сменным элементом шифра и используется для преобразования данного сообщения или данной совокупности сообщений; ключ шифрования формируется по детерминированным процедурам по секретному ключу; в ряде шифров в качестве ключа шифрования используется непосредственно секретный ключ;

- шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием шифрключа; шифр может быть реализован в виде программы для ЭВМ или в виде отдельного электронного устройства;

- подключ представляет собой часть ключа шифрования, используемую на отдельных элементарных шагах шифрования;

- шифрование есть процесс, реализующий некоторый способ преобразования данных с использованием шифрключа, переводящий данные в криптограмму, представляющую собой псевдослучайную последовательность знаков, из которой получение информации без знания ключа шифрования практически невыполнимо;

- дешифрование есть процесс, обратный процедуре шифрования; дешифрование обеспечивает восстановление информации по криптограмме при знании ключа шифрования;

- криптостойкость является мерой надежности защиты информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации по криптограмме при знании алгоритма преобразования, но без знания ключа шифрования.

Известны способы блочного шифрования данных, см. например стандарт США DES [У.Диффи, М.Э.Хеллмэн. Защищенность и имитостойкость: Введение в криптографию// ТИИЭР. 1979. Т. 67. N. 3. С. 87-89], способ шифрования по патенту США N 5222139, от 22 июня 1993 г., шифр FEAL-1 и криптоалгоритм В-Crypt [С.Мафтик. Механизмы защиты в сетях ЭВМ.- М., Мир, 1993. С. 49-52]. В известных способах шифрование блоков данных выполняют путем формирования ключа шифрования в виде совокупности подключей, разбиения преобразуемого блока данных на подблоки и поочередного изменения последних с помощью операций подстановки, перестановки и арифметических операций, выполняемых над текущим подблоком и текущим подключом.

Однако, известные способы аналоги не обладают достаточной стойкостью к дифференциальному криптоанализу [Berson T.A. Differential Cryptanalysis Mod 2^{32} with application to MD5// EUROCRYPT'92. Hungary, May 24-28, 1992. Proceedings. P. 67-68], т.к. для всех входных блоков данных для заданного шага преобразования используется один и тот же подключ в неизменном виде.

Наиболее близким по своей технической сущности к заявляемому способу блочного шифрования является способ, описанный в Российском стандарте криптографической защиты данных [Стандарт СССР ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования]. Способ-прототип включает в себя формирование ключа шифрования в виде последовательности из 8 подключей длиной 32 бита, разбиении входного 64-битового блока данных на два 32-битовых подблока B_1 и B_2 и поочередном преобразовании подблоков. Один шаг преобразования подблока, например подблока B_2 , заключается в наложении на него текущего подключа Q_i , являющегося фиксированным для данного шага, с помощью операции сложения по модулю 2^{32} (\boxplus) в соответствии с формулой $B_2 := B_2 \boxplus Q_i$, где $:=$ — знак операции присваивания, $1 \leq i \leq 8$, после чего над полученным новым значением подблока B_2 выполняют операцию подстановки, затем операцию циклического сдвига влево на одиннадцать бит, т.е. на одиннадцать двоичных разрядов в сторону старших разрядов, а затем на полученное значение B_2 накладывают подблок B_1 с помощью операции поразрядного суммирования по модулю два (\oplus) в соответствии с формулой $B_2 := B_2 \oplus B_1$. Операция подстановки выполняется следующим образом. Подблок разбивается на 8 двоичных вектора длиной по 4 бит. Каждый двоичный вектор заменяется двоичным вектором из таблицы подстановок. Выбранные из таблицы подстановок 8 4-битовых вектора

объединяются в 32-битовый двоичный вектор, который и является выходным состоянием подблока после выполнения операции подстановки. Всего выполняется 32 аналогичных шага изменения подблоков, причем для всех преобразуемых входных блоков данных на фиксированном шаге преобразования подблоков используется один и тот же подключ с неизменным значением.

Однако, способ-прототип имеет недостатки, а именно, при программной реализации он не обеспечивает скорость шифрования более 1 Мбит/с [Андреев Н.Н. О некоторых направлениях исследований в области защиты информации//Сборник материалов международной конференции 'Безопасность информации'. Москва, 14-18 апреля 1997. М. 1997. С. 96], что не позволяет использовать его для шифрования данных в средствах защиты реального масштаба времени. Этот недостаток связан с тем, что для обеспечения стойкости к дифференциальному криптоанализу в способе прототипе используется большое число операций подстановки над 4-битовыми подблоками преобразуемого блока данных, для выполнения каждой из которых (при программной реализации) микропроцессор осуществляет много элементарных команд, что обусловлено несоответствием подстановок такого типа с форматом представления данных в ЭВМ.

В основу изобретения положена задача разработать способ шифрования, в котором преобразование входных данных осуществлялось бы таким образом, чтобы обеспечивалось уменьшение числа элементарных операций преобразования, приходящихся на один бит входных данных, при одновременном обеспечении высокой стойкости к дифференциальному криптоанализу, благодаря чему повышается скорость шифрования при программной реализации.

Поставленная задача достигается тем, что в способе блочного шифрования дискретной информации, включающем формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом новым согласно изобретению является то, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию циклического сдвига, зависящую от j -того подблока, где $j \neq i$.

Благодаря такому решению структура подключей, используемых на заданном шаге шифрования, зависит от преобразуемых данных и тем самым на данном шаге преобразования для различных входных блоков используются различные модифицированные значения подключей, благо-

даря чему обеспечивается высокая стойкость к дифференциальному криптоанализу при одновременном уменьшении числа выполняемых операций преобразования, что и обеспечивает повышение скорости криптографического преобразования.

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи.

Изобретение поясняется обобщенной схемой криптографического преобразования блоков данных на основе заявляемого способа, которая представлена фиг. 1, где: операционный блок ОЦС — блок управляемой операции циклического сдвига; A и B — преобразуемые n -битовые подблоки; K_{2r} , K_{2r-1} — элементы ключа шифрования (подключи); знак \oplus обозначает операцию поразрядного суммирования по модулю два, знак \boxplus — операцию суммирования по модулю 2^n . Жирные сплошные линии обозначают шину передачи n -битовых сигналов, а жирные пунктирные линии — шину передачи n управляющих сигналов, в качестве которых используются биты преобразуемых подблоков.

Фиг. 1 показывает один (r -тый) раунд шифрования. В зависимости требуемой скорости преобразований могут быть заданы от 8 до 30 и более раундов.

Рассмотрим конкретные примеры реализации заявляемого способа криптографических преобразований блоков двоичных данных.

Пример 1.

В данном примере поясняется шифрование 64-битовых блоков данных. Ключ шифрования формируется в виде 16 подключей $K_1, K_2, K_3, \dots, K_{32}$, каждый из которых имеет длину 32 бит. Входной блок данных разбивается на два 32-битовых подблока A и B . Шифрование входного блока описывается следующим алгоритмом:

1. Установить счетчик числа раундов $r = 1$.
2. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus (K_{2r} \lll A),$$

где $K_{2r} \lll A$ обозначает операцию циклического сдвига влево на A бит, выполняемую над подключом K_{2r} .

3. Преобразовать подблок A в соответствии с выражением:

$$A := A \boxplus B,$$

где \boxplus — операция суммирования по модулю 2^{32} .

4. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus (K_{2r-1} \lll B),$$

где $K_{2r-1} \lll B$ обозначает операцию циклического сдвига влево на B бит, выполняемую над подключом K_{2r-1} .

5. Преобразовать подблок B в соответствии с выражением:

$$B := B \boxplus A.$$


6. Если $r \neq 16$, то прирастить счетчик $r := r + 1$ и перейти к шагу 2, в противном случае СТОП.


Современные микропроцессоры быстро осуществляют операцию циклического сдвига, в зависимости от значения переменной, хранящейся в одном из регистров. Благодаря этому описанный алгоритм обеспечивает скорость шифрования около 30 Мбит/с для массового микропроцессора Pentium/200.

Приведенные примеры показывают, что предлагаемый способ блочного шифрования дискретной информации технически реализуем и позволяет решить поставленную задачу.

Заявляемый способ может быть реализован, например, в виде программ для ЭВМ, обеспечивающих скоростное шифрование данных.

Авторы:  Масловский В.М.

 Молдовян А.А.

 Молдовян Н.А.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Способ блочного шифрования дискретной информации, включающий формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом, отличающийся тем, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию циклического сдвига, зависящую от j -того подблока, где $j \neq i$.

Авторы:



Масловский В.М.

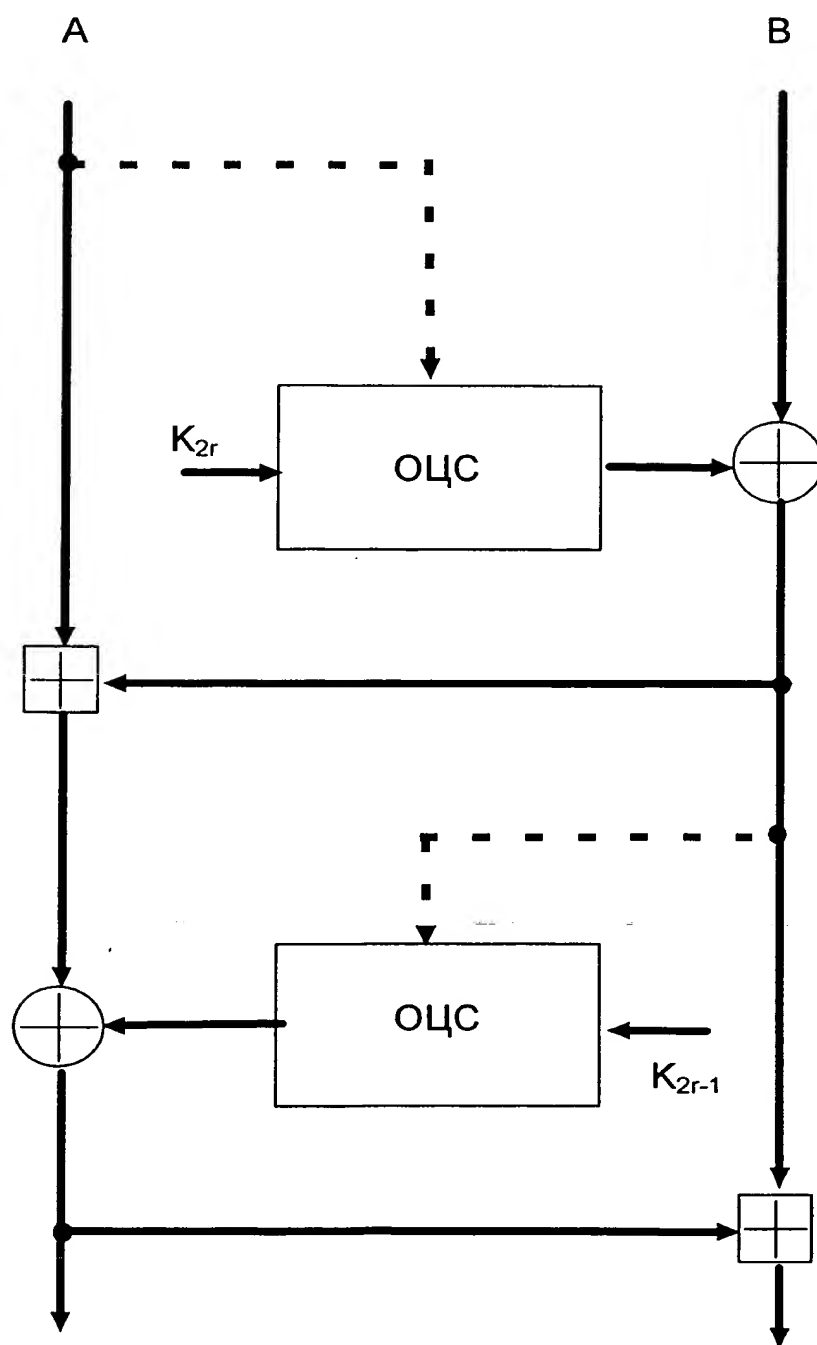


Молдовян А.А.



Молдовян Н.А.

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНОЙ ИНФОРМАЦИИ



Фиг.1.

Экз. N

РЕФЕРАТ

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Способ блочного шифрования дискретных данных, включающий формирование ключа шифрования

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования данных.

Целью изобретения является повышения скорости шифрования.

Способ включает формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом. Отличается от известных способов тем, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию циклического сдвига, зависящую от j -того подблока, где $j \neq i$.

Ф.и.-1, Илл.- 1.

THIS PAGE BLANK (USPTO)